April 8, 2004

E-MAIL SCAM USES "COPYCAT" WEB PAGES TO TRICK CONSUMERS

BISMARCK – Consumers in North Dakota should beware of e-mails that appear to be from national credit card and banking companies asking for verification of account information, warns Attorney General Wayne Stenehjem.

The scam emails, which look official, may have "Verify Your Identity," "Security Alert" or "Security Update" in the subject line. Most recent versions of the e-mail claim to be from "Citibank" and "PayPal," although scammers have used the names of other well-known national companies.

The high-tech scam, known as "phishing," uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other personal information.

The e-mails claim the company has updated its security system, and ask the consumer to confirm account information, verify the identity of the account holder, or confirm the e-mail address. A few of the "notices" even warn the account will be closed unless the information is verified.

"Consumers should be very cautious about responding to unsolicited e-mails. Consumers should call the company claiming to have sent the e-mail at a phone number obtained from a source other than the e-mail, or contact the Consumer Protection Division before responding to a suspicious e-mail," said Stenehjem.

Some emails include an embedded link to a fake secure website, while others contain a form for the consumer to complete and send. In both instances, the consumer is actually taken to a "copycat" website set up by the scammer. These "copycat" websites look exactly the same as the authentic website for the company mentioned in the scam e-mail, to trick the consumer.

The Attorney General's office provides the following tips for consumers:

- If you have an existing account with the company, call the customer service number listed on the credit card or account statement, instead of responding to the e-mail.
- Never "click" on the link included in the e-mail. Instead, start your Internet browser over again and type the company's web address into the browser. The web address is usually listed on the company letterhead and statements.
- Do not reply or respond to the e-mail – instead, delete it.

If you have replied to this e-mail, contact your bank or credit card company immediately. For information regarding this scam, or consumer information about identity theft, contact the Consumer Protection Division at 1-800-472-2600, or the Federal Trade Commission's identity theft website at www.consumer.gov/idtheft.

# # #